UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN VANCE, et al., Plaintiffs, v. MICROSOFT CORPORATION, Defendant.	CASE NO. C20-1082JLR ORDER GRANTING IN PART AND DENYING IN PART MICROSOFT'S MOTION TO DISMISS

I. INTRODUCTION

Before the court is Defendant Microsoft Corporation's ("Microsoft") motion to dismiss Plaintiffs Steven Vance and Tim Janecyk's (collectively, "Plaintiffs") complaint. (MTD (Dkt. # 25); Reply (Dkt. # 34).) Plaintiffs oppose the motion. (Resp. (Dkt. # 37).) Having considered the motion, the parties' submissions regarding the motion, the

//

//

//

relevant portions of the record, and the applicable law,[1] the court GRANTS in part and DENIES in part the motion to dismiss.

II. BACKGROUND

Facial recognition technology uses computer artificial intelligence and machine learning algorithms to "detect, recognize, verify and understand characteristics of humans faces."[2] (Compl. (Dkt. # 1) ¶ 23 (quoting Michele Merler, *et al.*, *Diversity in Faces*, IBM Research AI at 1 (Apr. 10, 2019)) ("*Diversity in Faces*").) However, "significant technical hurdles" hinder the technology's accuracy, and improving that accuracy relies upon "the use of data-driven deep learning to train increasingly accurate models by using growing amounts of data." (*Diversity in Faces* at 1.) In other words, practice makes perfect: for artificial intelligence to more accurately recognize different faces, "vast quantities of images of a diverse array of faces" must be fed to the underlying machine-learning algorithms. (Compl. ¶ 24.)

Microsoft is one of many companies that have developed and produced facial recognition products. (*Id.* ¶¶ 3, 52-53.) Among these products are its Cognitive Services Face Application Program Interface and its Face Artificial Intelligence service that allow customers to embed facial recognition technology into their applications. (*Id.* ¶ 53.) Microsoft conducts "extensive business within Illinois" related to facial recognition,

[1] Both parties request oral argument (MTD at 1; Resp. at 1), but the court finds oral argument unnecessary to its disposition of the motion, *see* Local Rules W.D. Wash. LCR 7(b)(4).

[2] For the purposes of a motion to dismiss, the court accepts all well-pleaded allegations in Plaintiffs' complaint as true and draws all reasonable inferences in favor of Plaintiffs. *See Wyler Summit P'ship v. Turner Broad. Sys., Inc.*, 135 F.3d 658, 661 (9th Cir. 1998).

including selling its facial recognition products through an Illinois-based vendor; working with an Illinois-based business to build new applications for facial recognition technology; and working with Illinois entities to build a "digital transformation institute" that accelerates the use of artificial intelligence throughout society. (*Id.* ¶ 59.)

Plaintiffs are Illinois residents who, starting in 2008, uploaded photos of themselves to the photo-sharing website Flickr. (*Id.* ¶¶ 6-7, 28, 60-61, 69.) Both were in Illinois when uploading the photos. (*Id.* ¶¶ 60, 69.) Unbeknownst to Plaintiffs, Flickr, through its parent company Yahoo!, compiled hundreds of millions of photographs posted on its platform, including those of Plaintiffs and other Illinois residents, into a dataset ("Flickr dataset") that it then made publicly available to "help improve the accuracy and reliability of facial recognition technology." (*Id.* ¶¶ 29-32.)

Utilizing the Flickr dataset, International Business Machines Corporation ("IBM") selected one million images to create a new dataset called Diversity in Faces in an effort to reduce bias in facial recognition. (*Id.* ¶ 40.) IBM scanned the "facial geometry" of the images and created a "comprehensive set of annotations of intrinsic facial features," including craniofacial distances, areas and ratios, facial symmetry and contrast, skin color, age and gender predictions, subjective annotations, and pose and resolution. (*Id.* ¶ 41 (citing *Diversity in Faces* at 2).) Ultimately, IBM utilized "19 facial landmark points" to determine "68 key points for each face" and to extract "craniofacial features" for each image in the dataset. (*Id.* ¶¶ 42-43 (citing *Diversity in Faces* at 9).) Again, the Diversity in Faces dataset included the facial scans of Plaintiffs and other Illinois

//

residents, but like Flickr and Yahoo!, IBM did not seek or receive permission from individuals whose faces were analyzed. (*Id.* ¶¶ 44-45.)

IBM made the Diversity in Faces dataset available to other companies seeking to improve their facial recognition technology. (*Id.* ¶ 47.) To obtain the dataset, companies applied for permission via an online questionnaire, and if IBM granted access, IBM would send a link for companies to download the dataset. (*Id.* ¶ 48.) Those with the dataset, and the corresponding information, could "identify the Flickr user who uploaded the photograph," "view the Flickr user's homepage," and "view each photograph's metadata, including any available [information] relating to where the photograph was taken or uploaded." (*Id.* ¶ 51.) Microsoft applied for and downloaded the dataset from IBM. (*Id.* ¶ 55.) Microsoft used the dataset to improve "the fairness and accuracy of its facial recognition products," which "improve[d] the effectiveness" of those products and made them "more valuable in the commercial marketplace." (*Id.* ¶¶ 57-58.) Once again, the dataset downloaded by Microsoft contained Plaintiffs' information, but Microsoft did not inform or obtain permission from Plaintiffs. (*Id.* ¶¶ 56, 65-66, 73-74.)

Plaintiffs bring a class action suit against Microsoft for violating Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which regulates the collection, storage and use of biometric identifiers and biometric information (collectively, "biometric data"). (*Id.* ¶¶ 4, 17.) Specifically, they allege violations of two BIPA provisions: (1) Microsoft violated § 15(b) by collecting and obtaining biometric data without providing the requisite information or obtaining written releases; and (2) Microsoft violated § 15(c) by unlawfully profiting from individuals' biometric data. (*Id.*

¶¶ 93-106.) Plaintiffs additionally bring an unjust enrichment claim (*id.* ¶¶ 107-16) and a separate count for injunctive relief (*id.* ¶¶ 117-22).

III. ANALYSIS

When considering a motion to dismiss under Rule 12(b)(6), the court construes the complaint in the light most favorable to the nonmoving party. *Livid Holdings Ltd. v. Salomon Smith Barney, Inc.*, 416 F.3d 940, 946 (9th Cir. 2005). The court must accept all well-pleaded facts as true and draw all reasonable inferences in favor of the plaintiff. *Wyler Summit P'ship*, 135 F.3d at 661. The court, however, is not required "to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)); *see also Telesaurus VPC, LLC v. Power*, 623 F.3d 998, 1003 (9th Cir. 2010). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 677-78. Dismissal under Rule 12(b)(6) can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory. *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990).

Microsoft moves to dismiss all of Plaintiffs' claims in its instant motion. (*See* MTD.) The court addresses the arguments pertaining to each claim in turn.

A. BIPA Claims

In urging the court to dismiss Plaintiffs' two BIPA claims, Microsoft first challenges the applicability of BIPA. (MTD at 6-15.) It argues that BIPA does not have extraterritorial effect here and that if it did, BIPA would violate the Dormant Commerce Clause. (*Id.*) Even if BIPA applies, Microsoft contends that Plaintiffs fail to state a claim. (*Id.* at 16-22.) The court addresses each argument in turn.

1. Illinois Extraterritorial Doctrine

Microsoft first argues that BIPA was not intended to have exterritorial effect and thus could not apply here because Plaintiffs have not established that the claim occurred in Illinois. (*Id.* at 6-9.) The court, like many others that have considered this argument, determines that at this early stage, it cannot dismiss the BIPA claims on this basis.

The parties agree that an Illinois statute does not have an "extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mutual Auto. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005); (MTD at 6; *see* Resp. at 4-5.) They further agree that BIPA does not have such an express provision and thus is not authorized to have extraterritorial effect. (MTD at 6; *see* Resp. at 4-5); *see Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017). Nonetheless, Plaintiffs may assert BIPA claims if they sufficiently allege that Microsoft's purported violations "occur[red] primarily and substantially in Illinois." *See Avery*, 835 N.E.2d at 853. The parties disagree on whether Plaintiffs have done so.

There is "no single formula or bright-line test for determining whether a transaction occurs within [Illinois]." *Id.* at 854. Instead, "each case must be decided on

its own facts." *Id.* Courts consider a myriad of factors, including the plaintiff's residency, the location of harm, where communications between parties occurred, and where a company is carrying out the aggrieved policy. *Id.* For transactions occurring on the Internet, courts may need to consider Internet-specific factors, such as where the site or information was accessed, or where the corporation operates the online practice. *See Rivera*, 238 F. Supp. 3d at 1101. As illustrated by these factors, whether events occurred primarily and substantially in Illinois is a "highly fact-based analysis that is generally inappropriate for the motion to dismiss stage." *Vance v. IBM Corp.*, No. 20 C 577, 2020 WL 5530134, at *3 (N.D. Ill. Sept. 15, 2020) ("*IBM*").

Accordingly, the majority of courts in BIPA cases to consider the issue at this stage have denied the motion to dismiss, opting instead to allow discovery for more information regarding the extent to which the alleged misconduct occurred in Illinois. *See, e.g.*, *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017); *cf. In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547-48 (N.D. Cal. 2018) (analyzing issue in class certification context). In *Rivera*, the plaintiffs alleged that they were Illinois residents; that their photographs were taken and uploaded in Illinois; and that the defendant failed to provide the required disclosures in Illinois, but they did not allege where the defendant accessed their photographs or facial scans. 238 F. Supp. 3d at 1101-02. Nonetheless, the court concluded that the allegations "tip[ped] toward a holding that the alleged violations primarily happened in Illinois." *Id.* However, the court recognized the need for discovery, highlighting the need for more information regarding where the injury and the lack of consent took place. *Id.* at 1102.

The court holds the same based on Plaintiffs' allegations. Plaintiffs, and all purported class members, are Illinois residents who, while in Illinois, uploaded photos that were taken in Illinois. (Compl. ¶¶ 6-7, 60-61, 69.) The required disclosures or permissions would have been obtained from Illinois, and so any communication would have necessarily involved Illinois. (*See id.* ¶¶ 65-66, 73-74.) The alleged harm to privacy interests is ongoing for Illinois residents. (*Id.* ¶¶ 67, 75, 77.) Moreover, Plaintiffs allege that Microsoft conducts "extensive business" in Illinois involving their facial recognition products (*id.* ¶ 59), and that the Diversity in Faces dataset "improve[d] its facial recognition products" (*id.* ¶ 58), thereby allowing the reasonable inference that Microsoft utilized the dataset in Illinois during its business dealings.

While Microsoft is correct that Plaintiffs do not allege where Microsoft obtained the dataset (*see* MTD at 7), that fact alone may not be dispositive. *See Rivera*, 238 F. Supp. 3d at 1102 (citing *Avery*, 835 N.E.2d at 853). It is certainly possible that with more factual refinement around this complex issue, the circumstances around Microsoft's attainment, possession and use of the Diversity in Faces dataset will reveal that the alleged violations did not occur primarily in Illinois. *See IBM*, 2020 WL 5530134, at *3. But more information is needed to reach any determination, and so, the court agrees with *Rivera* that "[f]or now, it is enough to say that the allegations survive the accusation that the law is being applied outside of Illinois." *See* 238 F. Supp. 3d at 1102.

Microsoft attempts to distinguish those previous cases by arguing that they involve plaintiffs who "uploaded a photo directly to the defendant's systems," whereas Plaintiffs did not upload anything directly to Microsoft's systems. (MTD at 8 (bolding and italics

removed).) This argument is unavailing for two reasons. First, Microsoft's distinction does not hold true for all cases. In *IBM*—a suit brought by Plaintiffs against IBM for its part in this chain—the court found dismissal premature even though Plaintiffs did not upload anything directly to IBM's systems. *See* 2020 WL 5530134, at *3; *see also Monroy*, 2017 WL 4099846, at *1-2, 6 (identifying plaintiff as non-Illinois resident who "does not use Shutterfly"). The fact that Plaintiffs did not access any IBM products had no impact on how "discovery is needed in order to determine to what extent IBM's alleged acts occurred in Illinois." *IBM*, 2020 WL 5530134, at *3. Second, direct upload is not the only way to establish that an alleged violation occurred in Illinois, and Microsoft points to no authority saying so. (*See* MTD.) Thus, while Microsoft is correct that Plaintiffs' connection with Microsoft—and in turn, the connection between the alleged misconduct and Illinois—is not through direct use of its products, that does not defeat the need for more information that may bear on this fact-laden analysis.

The authority Microsoft relies upon are easily distinguishable. In *Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088 (N.D. Ill. 2019), the plaintiff did not allege that her biometric information was collected in Illinois, and thus, the court could not reasonably infer any connection with Illinois.[3] *Id.* at 1091. Plaintiffs here have explicitly pleaded their connection with Illinois. (Compl. ¶¶ 6-7, 60-61, 69.) Similarly, in *Tarzian v. Kraft*

//

[3] Like Microsoft, the defendant in *Neals* was a non-resident corporation with no allegations that it had property or stored data in Illinois. 419 F. Supp. 3d at 1091. The court made clear that the defendant's "physical location and property holdings, the location of its servers, and the identity of its customers [who used its technology to collect biometric information] are not determinative of [BIPA's] application." *Id.*

Heinz Foods Co., No. 18 C 7148, 2019 WL 5064732 (N.D. Ill. Oct. 9, 2019), the court dismissed consumer fraud claims brought by non-resident plaintiffs when the only connection to Illinois was that the deception scheme allegedly originated there. *Id.* at *3. Notably, the same claims brought by resident plaintiffs survived. *See id.* Plaintiffs here have pleaded many more allegations than the non-residents in *Tarzian*, including their own residency and Illinois as the place of harm. (Compl. ¶¶ 60-62, 68-70, 77.)

In sum, more discovery is needed to explore whether and to what extent Microsoft's alleged acts involving the Diversity in Faces dataset occurred in Illinois. For now, Plaintiffs' allegations are sufficient to withstand dismissal.

2. Dormant Commerce Clause

Building on its extraterritoriality argument, Microsoft next argues that applying BIPA as Plaintiffs allege here would violate the Dormant Commerce Clause. (MTD at 9-15.) Specifically, because Microsoft maintains that it has not "engaged in any relevant conduct in Illinois," it contends that Plaintiffs' BIPA claims would allow Illinois law to control transactions outside its boundaries. (*Id.* at 10 (bolding and italics removed).)

The Commerce Clause has "long been understood to have a 'negative' aspect that denies the States the power unjustifiably to discriminate against or burden the interstate flow of articles of commerce," known as the Dormant Commerce Clause. *Or. Waste Sys., Inc. v. Dep't of Env't Quality of State of Or.*, 511 U.S. 93, 98 (1994); *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614 (9th Cir. 2018). A state statute runs afoul of the Dormant Commerce Clause if it "directly regulate[s]" interstate commerce by "affect[ing] transactions that take place across state lines or entirely outside the state's

borders." *Daniels Sharpsmart*, 889 F.3d at 614. Thus, the Dormant Commerce Clause prohibits "the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State." *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989).

As many courts have observed, the Dormant Commerce Clause argument is directly related to the extraterritoriality effect argument, as both hinge on where the alleged misconduct takes place. *See In re Facebook*, 2018 WL 2197546, at *4. Thus, unsurprisingly, most courts in this context have found that the Dormant Commerce Clause argument is "more properly addressed on a motion for summary judgment." *See, e.g.*, *IBM*, 2020 WL 5530134, at *4. In *IBM*, the court concluded that it "need[s] more detailed facts regarding IBM's processes to know the extent to which IBM's actions occurred in Illinois and whether the Dormant Commerce Clause bars this suit." *Id.*; *see also Rivera*, 238 F. Supp. 3d at 1104 ("Whether the [BIPA] is nevertheless being summoned here to control commercial conduct wholly outside Illinois is not possible to figure out without a better factual understanding of what is happening in the Google Photos face-scan process."); *Monroy*, 2017 WL 4099846, at *8 (stating that "important information is lacking regarding how Shutterfly's technology works").

Again, the court agrees with those that have previously considered the issue. At this point, the court needs more information about the technology behind how Microsoft obtained, stores, or uses the Diversity in Faces dataset to conclude that applying BIPA would run afoul of the Dormant Commerce Clause. Nor does the court have an adequate basis for determining whether applying BIPA here would, as Microsoft argues, displace

the policies of other states. (*See* MTD at 12-15.) As discussed above, the fact that Plaintiffs did not directly interact with Microsoft's systems does not affect the need for more detailed facts about Microsoft's processes. *See IBM*, 2020 WL 5530134 at *3-4. Accordingly, the court denies Microsoft's motion to dismiss on applicability grounds.

3. Failure to State a Claim

Finally, Microsoft contends that Plaintiffs fail to state a claim for three reasons. (MTD at 16-22.) Microsoft first maintains that BIPA does not apply to photographs, and thus, Plaintiffs cannot bring a claim under either §§ 15(b) or 15(c) for facial scans derived from their photographs. (*Id.* at 16-19.) Alternatively, Microsoft argues that § 15(b) only applies to "entities who actively 'collect'" biometric data and that § 15(c) only applies to "the direct provision of biometric data in exchange for money"—neither of which are alleged here. (*Id.* at 19-22.) The court disagrees and reviews each contention in turn.

a. BIPA's Applicability to Photographs

BIPA prohibits private entities from gathering or using "biometric identifier[s]" or "biometric information" without notice and consent. 740 ILCS 14/15. A "[b]iometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. Biometric identifiers "do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." *Id.* "Biometric information" means "any information . . . based on an individual's biometric identifier used to identify an individual" but "does not include information derived from items . . . excluded under the

definition of biometric identifiers." *Id.* Microsoft reasons that because photographs are not "biometric identifiers," and "biometric information" does not include information derived from photographs, Plaintiffs' facial scans created from their photographs do not qualify as either biometric identifiers or biometric information. (MTD at 16.) The court disagrees and holds that the facial scans are "biometric identifiers" under BIPA.

This is not the first—or second, or third, or even fourth—time that defendants have challenged BIPA's applicability to facial scans derived from photographs. Every court has rejected Microsoft's argument.[4] *See, e.g.*, *Monroy*, 2017 WL 4099846, at *3 (calling defendant's reading "sensible enough at first blush" but concluding "it begins to unravel under scrutiny"). The reason lies in the statute's plain language, where the statutory interpretation analysis must begin. *See Lacey v. Village of Palatine*, 904 N.E.2d 18, 25 (Ill. 2009). The court gives the language its plain and ordinary meaning. *Hadley v. Ill. Dep't of Corrections*, 864 N.E.2d 162, 165 (Ill. 2007). When the language is clear, it will be given effect without resort to other aids of construction. *Id.* The court may not "under the guise of construction, supply omissions, remedy defects, annex new provisions, substitute different provisions, and exceptions, limitations or conditions, or otherwise change law so as to depart from the language employed in the statute." *DeWig v. Landshire, Inc.*, 666 N.E.2d 1204, 1207 (Ill. App. Ct. 1996).

[4] Recognizing the weight of authority against it, Microsoft maintains that all those cases were wrongly decided. (MTD at 17-18.) For instance, Microsoft states that *Rivera* did not "properly account for BIPA Section 5," which lists only in-person transactions as examples that are regulated. (*Id.* at 18.) Not so. *See Rivera*, 238 F.3d at 1098 (analyzing Section 5 and its list of example transactions). Microsoft has not offered persuasive arguments that *Rivera* and other cases were wrongly decided.

Here, the "comprehensive set of annotations of intrinsic facial features" (Compl. ¶ 41) is one of the biometric identifiers listed in BIPA's plain text: a "scan of . . . face geometry," 740 ILCS 14/10; *see, e.g.*, *Rivera*, 238 F. Supp. 3d at 1095 ("[E]ach face template . . . [features] a set of biology-based measurements ('biometric') that is used to identify a person ('identifier')."). Plaintiffs "do not claim that simply possessing a photograph of a face violates BIPA," and thus the exclusion of photographs as biometric identifiers has little bearing. (*See* Resp. at 15 n.4.) And while these facial scans may not qualify as biometric information—because they are "derived from items . . . excluded under the definition of biometric identifiers," namely, photographs—there is no textual support for the contention that these scans could not be biometric identifiers themselves. *See* 740 ILCS 14/10; *In re Facebook*, 185 F. Supp. 3d at 1171 (finding "digital representation of the face . . . based on geometric relationship of their facial features" to be a "scan of face geometry").

At base, Microsoft takes issue with how these scans are captured. It argues that only scans taken in-person, not from photographs, are biometric identifiers. (*See* MTD at 18.) Put another way, Microsoft wishes to apply the same limitation that is placed on biometric information to biometric identifiers. *See* 740 ILCS 14/10. But the Illinois legislature chose not to use terms such as "derived from" when defining biometric identifier. *See Rivera*, 238 F. Supp. 3d at 1097 ("It would have been simple enough for the Illinois legislature to include similar 'based on' or 'derived from' language in the definition of 'biometric identifier' but it did not."); *see also Dana Tank Container, Inc. v. Hum. Rts. Comm'n*, 687 N.E.2d 102, 104 (Ill. App. Ct. 1997) ("Where the legislature

uses certain words in one instance and different words in another, it intended different results."). "The bottom line is that a 'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component . . . used to identify a person." *Rivera*, 238 F. Supp. 3d at 1097. The facial scans here fall squarely within that definition.[5] Accordingly, the court denies Microsoft's motion to dismiss the BIPA claims on this ground.

b. Obtaining Biometric Data Under § 15(b)

Microsoft argues next that § 15(b) of BIPA is only triggered by those who "actively 'collect'" biometric data, whereas it "merely 'possess[es]'" the data. (MTD at 19-21.) Plaintiffs respond that the complaint contains sufficient allegations to establish how Microsoft obtained and used their biometric data, contending that Microsoft "could not have used the [data] unless it first collected or obtained it." (Resp. at 18.) The court agrees with Plaintiffs.

Again, the analysis begins, and ends, with BIPA's plain language. The protections under § 15(b) are triggered whenever a private entity "collect[s], capture[s], purchase[s], receive[s] through trade, or otherwise obtain[s]" biometric data. 740 ILCS 14/15(b). The catch-all phrase "otherwise obtain" is not defined by BIPA. *See* 740 ILCS 14/10. Where a term is undefined, "[i]t is entirely appropriate to employ the dictionary as a resource to ascertain [its] meaning." *Lacey*, 904 N.E.2d at 26. "Obtain" is defined as "[t]o come into

[5] Because the text is "plain and unambiguous," the court need not consider Microsoft's legislative history arguments. *See Ultsch v. Ill. Mun. Ret. Fund*, 874 N.E.2d 1, 10 (Ill. 2007). Even if the court considered them, it finds persuasive the *Rivera* court's analysis and ultimate rejection of similar arguments. *See* 238 F. Supp. 3d at 1098-100.

the possession of," or "to get, acquire, or secure." *Obtain*, Oxford English Dictionary, https://www.oed.com/view/Entry/130002 (last visited Mar. 9, 2021). "Otherwise" means "[i]n a different manner; in another way, or in other ways." Black's Law Dictionary 1101 (6th ed. 1990); *see also Otherwise*, Oxford English Dictionary, https://www.oed.com/view/Entry/133247 (last visited Mar. 9, 2021). Accordingly, in context, § 15(b) is triggered whenever a private entity acquires biometric data in the enumerated ways—collecting, capturing, purchasing, receiving through trade—or gets the biometric data in some other way.

Plaintiffs have sufficiently alleged that Microsoft got its biometric data in some other way—namely by applying for and downloading the data set from IBM. (*See* Compl. ¶¶ 55-57.) Moreover, Plaintiffs allege that Microsoft used the biometric data to "improve its facial recognition products and technologies." (*Id.* ¶¶ 57-58.) Contrary to Microsoft's contentions, these allegations establish more than "passive 'possession.'" (*See* MTD at 20.) Indeed, Microsoft does not explain how it could have come into possession of or used Plaintiffs' facial scans without having first obtained it. *See Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 784 (N.D. Ill. 2020) ("[T]o have [stored or used] the data, [the defendant] necessarily first had to 'obtain' the data."). Thus, it makes no difference that § 15(b) does not contain the word "possession" whereas the other provisions do, because even accepting Microsoft's argument that "only actions trigger [§] 15(b)," Plaintiffs have sufficiently alleged such actions.[6] (*See* MTD at 20.)

[6] Obtaining biometric data via a download could also qualify as "collecting" that data. *See Collect*, Oxford English Dictionary, https://www.oed.com/view/Entry/36263 (last visited

Nor will the court adopt Microsoft's proposal that § 15(b) only applies when an entity acquires biometric data "directly from any individual." (*See* MTD at 20.) Nothing in the statute's language supports such a narrow application. For instance, the word "collect" carries no inherent limitation on who or where the information is collected from. *See Collect*, Oxford English Dictionary, https://www.oed.com/view/Entry/36263 (last visited Mar. 9, 2021) (defining "collect" simply as "to gather"). Section 15(b) does not add any limitation either, stating only that the protections are triggered when an entity collects biometric data, regardless of how that collection occurs. *See* 740 ILCS § 15(b). The same is true of the other methods of attainment in the provision. In essence, Microsoft wishes the court to read the limitation "directly from the person" into § 15(b) where none exists. The court cannot do so. *See DeWig*, 666 N.E.2d at 1207.

This straightforward reading of the text does not, as Microsoft fears, produce an absurd result. (*See* MTD at 20-21.) BIPA obligates any private entity that obtains a person's biometric identifier to comply with certain requirements to protect that person's privacy interests. *See* 740 ILCS 14/5 (recognizing public's wariness of use of biometrics and need for regulation for public welfare, security and safety). Whether that biometric information comes from an individual or is part of a large dataset, there is nothing absurd about requiring any entity that obtains such information to comply with the safeguards

//

//

Mar. 9, 2021) (defining "collect" as "to gather together"). Because the court finds that Microsoft's actions qualify under "otherwise obtain," it need not determine whether these actions could also fall with the meaning of the enumerated terms.

that the Illinois legislature deemed necessary.[7] *See Neals*, 419 F. Supp. 3d at 1092; 740 ILCS 14/5(g). Although complying with BIPA requires entities like Microsoft to take additional steps before acquiring biometric data, the court does not believe that "under Plaintiffs' reading of the statute, no entity could safely download any large biometric dataset." (*See* MTD at 21 (bolding and italics removed).)

Microsoft relies solely on cases in the employment context (*see id.* at 20), and the court acknowledges that there is a "split on . . . whether BIPA governs outside vendors" who provide biometric timekeeping systems to employers, *see Figueroa*, 454 F. Supp. 3d at 783-84. Analogizing itself to these third-party vendors, Microsoft argues that it also has no relationship with those whose facial scans are in the dataset. The court is unpersuaded. As a preliminary matter, the court observes that most of these cases focus on, as expected, circumstances specific to employment and do not purport to extend beyond that context.[8] *See Cameron v. Polar Tech. Indus., Inc. & ADP, LLC*, No. 2019-CH-000013 (Ill. Cir. Ct. Aug. 23, 2019) at 33:22-34:3.[9] But more importantly, these cases concern complaints that do not sufficiently plead the role of the third-party, thus warranting dismissal. In *Namuwonge v. Kronos, Inc.*, the plaintiff alleged that only

//

[7] Indeed, it stands to reason that if the Illinois legislature were concerned about individual collection of biometric data that could compromise identity—which Microsoft seems to have no qualms with (*see* MTD at 20-21)—the legislature would be equally, if not more concerned about that data being shared in large swaths accessible through download.

[8] BIPA may very well treat the use of biometric data in employment differently, as the statute defines "written release" differently in the employment context. *See* 740 ILCS 14/10.

[9] Microsoft attaches the transcript of the *Cameron* court's oral ruling as an exhibit to its motion to dismiss. (*See* MTD, Ex. E.)

the employer, not the third-party vendor, obtained her fingerprints. 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019). Similarly, in *Bernal v. ADP, LLC*, No. 2017-CH-12364 (Ill. Cir. Ct. Aug. 23, 2019), the decision "ultimately turn[ed] on the insufficiency of [the] [p]laintiff's complaint" because he alleged only that the third-party vendor supplied the biometric technology. *Id.* at 3. The same is not true here. To the extent that dicta in these cases require some relationship to exist, the court declines to adopt that interpretation, as that requirement does not appear in the statutory language, and persuasive authority exists to the contrary. *See, e.g.*, *Flores v. Motorola Solutions, Inc.*, No. 1:20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021); *Monroy*, 2017 WL 4099846, at *1.

In sum, § 15(b) applies when a private entity collects, captures, purchases, trades for, or gets biometric data in some other way. Plaintiffs allege that Microsoft got the biometric data in some other way by applying for and downloading it from IBM and then used that data to improve its own products. (Compl. ¶¶ 48-49, 55-58.) Such allegations suffice to trigger § 15(b).

c. Profit Under § 15(c)

Lastly, Microsoft contends that § 15(c) of BIPA does not apply because Plaintiffs have not alleged that it has exchanged biometric data for a pecuniary benefit. (MTD at 21-22.) Section 15(c) states that no private entity may "sell, lease, trade, or otherwise profit from" the biometric data in its possession. 740 ILCS 14/15(c). Microsoft argues that sell, lease, trade, and profit "all contemplate the direct provision of biometric data in exchange for money," which doesn't reach the "indirect 'profit'" of improving its facial

//

recognition products. (MTD at 22.) The court determines that supplemental briefing is needed and thus defers ruling on the issue.

The question of what "otherwise profit from" means in § 15(c) is a novel issue. However, neither party spends more than a page briefing the issue, nor do they offer any authority analyzing this provision.[10] (*See* MTD at 21-22; Resp. at 22-23; Reply at 10-11.) The parties focus instead on the doctrine of *ejusdem generis* and whether it applies to verbs. (*See* MTD at 22; Resp. at 22; Reply at 11.) The court additionally recognizes that the parties' briefing was completed in the fall of 2020, and there is the possibility that more recent case law has analyzed this issue since that time. Thus, the court finds additional briefing would be beneficial and defers ruling on this issue. The court directs the parties to file responses to this order addressing the definition of "otherwise profit from" in the context of § 15(c), including an analysis of any recent case law that bears on the issue. The parties' responses for this issue and the choice-of-law issue, *see infra* § III.B, shall total no more than 15 pages and be filed by **Friday, March 26, 2021, at 5:00 p.m.** There shall be no replies unless otherwise ordered by the court.

B. Unjust Enrichment Claim

Microsoft next challenges Plaintiffs' unjust enrichment claim as insufficiently pleaded under Washington law. (MTD at 22-24.) Plaintiffs respond that the claim is

//

[10] The court acknowledges that Plaintiffs filed a Notice of Supplemental Authority identifying a recent case that may bear on this analysis. (*See* Not. of Supp. Authority (Dkt. # 35).) However, neither party has had a chance to meaningfully apply the identified case to the allegations here.

sufficiently pleaded under Illinois law. (Resp. at 23-24.) Thus, the court must resolve a choice-of-law question before determining whether the unjust enrichment claim survives.

A federal court sitting in diversity applies the choice-of-law rules of its forum state to determine which substantive law controls. *Kohlrautz v. Oilmen Participation Corp.*, 441 F.3d 827, 833 (9th Cir. 2006). Washington employs a two-step approach. *Kelley v. Microsoft Corp.*, 251 F.R.D. 544, 550 (W.D. Wash. 2008). First, the court must determine whether "an actual conflict between Washington and the other applicable state law exists." *Id.* (citing *Burnside v. Simpson Paper Co.*, 864 P.2d 937, 942 (1994)). If there is an actual conflict, then the court must determine which state has the "most significant relationship" to the action. *Id.* (citing *Johnson v. Spider Staging Corp.*, 555 P.2d 997, 1000 (Wash. 1976)).

An actual conflict between Washington and Illinois law exists over whether Plaintiffs must plead that they suffered an economic expense distinct from a privacy harm. An actual conflict exists when the two laws "could produce different outcomes on the same legal issue." *Id.* at 550. In Washington, alleging a non-economic loss, such as a loss of privacy, is insufficient because "Washington courts have not applied the doctrine of unjust enrichment outside the context of an 'expense' stemming from some tangible economic loss to a plaintiff." *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1130 (W.D. Wash. 2012). Plaintiffs make no argument why *Cousineau* is not controlling law in Washington. (*See* Resp. at 23-24.) In Illinois, however, the assertion that plaintiffs are "exposed to a heightened risk of privacy harm" and "have been deprived of their control

//

over their biometric data" sufficiently states an unjust enrichment claim. *Vance*, 2020 WL 5530134, at *5. Microsoft does not argue otherwise. (*See* MTD at 22-24; Reply at 12.) Because the two laws would produce different outcomes on this legal issue, the court determines that there is an actual conflict between Washington and Illinois law.

Because there is an actual conflict, the court must apply Washington's "most significant relationship" test to determine which law governs. *Coe v. Philips Oral Healthcare Inc.*, No. C13-0518MJP, 2014 WL 5162912, at *3 (W.D. Wash. Oct. 14, 2014). First, the court considers the states' relevant contacts to the cause of action, and if those contacts are balanced, the court must then consider "the interests and public policies of [the two] states and . . . the manner and extent of such policies as they relate to the transaction in issue." *Johnson*, 555 P.2d at 1001. This analysis can be complex, involving an identification of the relevant contacts, assigning significance to those contacts, and weighing those contacts. *See Kelley*, 251 F.R.D. at 551-53; *Coe*, 2014 WL 5162912, at *3-4; Restatement (Second) of Law on Conflict of Laws §§ 145-55. Moreover, some of the traditionally relevant contacts, such as where the injury and misconduct occurred, may concern facts that the court currently lacks. *See supra* § III.A.1-2. Despite the intricacies of this analysis, neither party meaningfully addresses the issue, nor do they offer analogous case law. (*See* MTD; Resp; Reply.)

The court concludes that further briefing from the parties on this issue would be beneficial. Accordingly, the court defers ruling on Microsoft's motion to dismiss Plaintiffs' unjust enrichment claim. The court further directs the parties to file responses to this order on the question of which state law should govern under Washington's "most

significant relationship" test. In particular, the parties should touch on how the contacts analysis differs, if at all, for an unjust enrichment claim in a privacy suit and address whether further factual development is needed to analyze the states' relevant contacts. The parties' responses addressing the choice-of-law issue and the aforementioned § 15(c) issue, *see supra* § III.A.3.c, shall total no more than 15 pages and be filed by **Friday, March 26, 2021, at 5:00 p.m**. There shall be no replies unless otherwise ordered.

C. Injunctive Relief

Lastly, Microsoft asserts that Plaintiffs' count for injunctive relief must be dismissed. (MTD at 24.) The court agrees that "[i]njunctive relief is a remedy, not a cause of action." *Edifecs Inc. v. TIBCO Software Inc.*, No. C10-0330RSM, 2011 WL 1045645, at *3 (W.D. Wash. 2011). Plaintiffs do not argue otherwise. (*See* Resp.) Accordingly, the court dismisses Plaintiffs' standalone injunctive relief claim, but Plaintiffs may pursue injunctive relief in connection with its other claims.

//

//

//

//

//

//

//

//

//

IV. CONCLUSION

For the foregoing reasons, the court GRANTS in part and DENIES in part Microsoft's motion to dismiss (Dkt. # 25). Specifically, the court GRANTS the motion to dismiss Plaintiffs' injunctive relief claim but DENIES the motion as it applies to Plaintiffs' BIPA § 15(b) claim. The court DEFERS ruling on Plaintiffs' BIPA § 15(c) and unjust enrichment claims and further DIRECTS the parties to file responses on those two issues as identified above. These responses shall not exceed 15 pages and must be filed by **Friday, March 26, 2021, at 5:00 p.m**.

Dated this 15th day of March, 2021.

JAMES L. ROBART
United States District Judge